

*AUSA Sproule*

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

IN THE MATTER OF THE  
APPLICATION FOR A SEARCH AND  
SEIZURE WARRANT FOR 1401  
MERCANTILE LANE, SUITE 200-CC,  
LARGO, MARYLAND

IN THE MATTER OF THE  
APPLICATION FOR A SEARCH AND  
SEIZURE WARRANT FOR AND 4312  
ARABELLA COURT, UPPER  
MARLBORO, MARYLAND AND

IN RE CRIMINAL COMPLAINT FOR  
SAUNDRA WHITE

Case No. *13-1187 JKS*

Under Seal

Case No. *13-1188 JKS*

Under Seal

Case No. *13-1189 JKS*

Under Seal

FILED  
LOGGED  
ENTERED  
RECEIVED  
MAY 15 2013  
CLERK AT GREENBELT  
U.S. DISTRICT COURT  
DISTRICT OF MARYLAND  
DEPUTY

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR  
SEARCH AND SEIZURE WARRANTS AND CRIMINAL COMPLAINT**

The affiant herein is John Davids, a Special Agent with the United States Treasury  
Inspector General for Tax Administration ("TIGTA"), who being duly sworn states as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with TIGTA, Baltimore Post-of-Duty. I have been a  
Criminal Investigator/Special Agent with this organization and its predecessor for 25 years.  
Prior to that, I was a Criminal Investigator/Special Agent with the U.S. Department of State,  
Diplomatic Security Service and a Police Officer with the Baltimore Police Department. I have  
graduated from the Federal Law Enforcement Training Center after completing the Criminal  
Investigator Training Program, the Advanced Investigation Techniques and the Baltimore City  
Police Academy.

2. I am duly commissioned as a Special Agent, and I am authorized to conduct criminal and other investigations arising under the laws of the United States. I am authorized to carry firearms, execute and serve search and arrest warrants. I have conducted and participated in numerous investigations of criminal violations involving Titles 18 and 26 of the United States Code, to include fraud, theft, computer crimes, impersonation, bribery, drug crimes, assaults and threats. I have executed or participated in the execution of approximately 100 search warrants during my career and have seized evidence in relation to criminal activity.

### **TARGET LOCATIONS**

3. This affidavit is submitted in support of the request for the issuance of a search and seizure warrant for the following premises:

- a. 1401 Mercantile Lane, Suite 200-CC, Largo, Maryland 20774, which is the office of SAUNDRA WHITE, possibly also doing business as Great White Bay, LLP, as further described in Attachment A; and
- b. 4312 Arabella Court, Upper Marlboro, Maryland 20774, which is the residence of SAUNDRA WHITE, as further described in Attachment B (together the "Target Locations").

4. The first listed premises to be searched, 1401 Mercantile Lane, Suite 200-CC, Largo, Maryland, 20774, is a portion of a seven-story office building that houses offices for businesses. Displayed on the top front of the office building are the numbers 1401 and below the numbers are glass windows down to the glass entrance doors. The office to be searched is located in Suite 200, on the second floor, directly to the right of the elevators. Suite 200 also contains numerous other businesses. Office 200-CC is located down the hallway directly to the right after entering Suite 200 and passing through a sitting area. Office 200-CC is identified by a

brown door and to the left of the door is a sign that has the numbers 200-CC. Directly below are the words "Great White Bay, LLP."

5. The second listed location to be searched, 4312 Arabella Court, Upper Marlboro, Maryland 20774, is a two-story, brick front single family residence located on the southeast corner of Arabella Court and Dunkirk Drive. The house has brown brick and cream trim, and the numbers 4312 are attached on the fascia over the front door, and when facing the house from the street, there are two cream colored garage doors on the left side of the house.

6. Based on the facts set forth below, your affiant respectfully submits there is probable cause to believe that there is presently contained within the above-described locations, files, correspondence, memoranda, computers, computer disks, bank and other financial records, cellular telephones, monies, and other materials that constitute evidence of, the fruits of, or instrumentalities of wire fraud, a violation of Title 18, United States Code, Section 1343; misuse of Department of Treasury names and symbols, a violation of Title 31, United States Code, Section 333, which criminalizes the use of words, symbols or emblems or imitations in connection with a business activity that falsely conveys endorsement or association with the Department of Treasury or any subdivisions thereof; and aggravated identity theft, a violation of Title 18, United States Code, Section 1028A (together, the "Target Offenses").

#### **CRIMINAL COMPLAINT**

7. Also, this affidavit is submitted in support of the request for the issuance of a criminal complaint because there is probable cause to believe that that SAUNDRA WHITE committed the Target Offenses.

8. The facts set forth herein reflect my personal knowledge gained in this investigation, including witness interviews and the review of documents and records obtained as

part of the investigation. The conclusions set forth herein are the product of that information, coupled with my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the issuance of the requested authorization to search the Target Locations and for the issuance of a criminal complaint and does not set forth all of my knowledge about this matter.

**PROBABLE CAUSE**

9. Your affiant has learned that taxpayer P.H. received numerous fraudulent notices that, from their face, purported to be from the Internal Revenue Service ("IRS"). The notices made demand for payments of back taxes regarding a distant family member for whom P.H. had legal guardianship, C.M. In response to these demand notices, P.H., at the direction of her attorney, SAUNDRA WHITE, mailed multiple cashier's checks to a post office box ("P.O. Box") in Annapolis, Maryland.

10. Your affiant examined the notices purportedly from the IRS and knows from his experience and training, and knowledge of certain features typical of official IRS documents, that these questioned notices are fraudulent.

11. On February 27 and March 1, 2013, I interviewed P.H., and she reported to me that on December 26, 2009, her cousin, C.M., had suffered a severe stroke and because she had no close relatives in the area, P.H. assumed responsibility for her care and wellbeing. She further reported that sometime in March of 2010, she contacted SAUNDRA LUCILLE WHITE and requested assistance with obtaining guardianship for C.M. WHITE attended the same church as P.H., and P.H. knew her to be an attorney.

12. WHITE agreed to assist P.H. in obtaining guardianship for C.M., and P.H. signed an "Engagement Agreement" for WHITE. WHITE asked P.H. if she could provide WHITE with



a quick accounting of C.M.'s assets. On April 5, 2010, P.H. faxed WHITE a document showing that C.M. had bank accounts and certificates of deposit totaling \$240,393.29.

13. P.H. received temporary guardianship in April of 2010 and then was awarded permanent guardianship on October 13, 2010. When P.H. received temporary guardianship, she gave WHITE a key to C.M.'s condominium and asked WHITE to assist with inventorying C.M.'s personal property. According to P.H., WHITE and her assistants made several trips to the condominium going through C.M.'s property.

14. Sometime in the spring of 2010, WHITE contacted P.H. and told her that she had a document she wanted to show her. When the two met, WHITE showed P.H. a Last Will and Testament that named P.H. and her mother as sole beneficiaries of C.M.'s estate.

15. In June of 2010, WHITE asked P.H. several times if she was picking up C.M.'s mail. On or about the second week of June 2010, P.H. picked up C.M.'s mail at C.M.'s condominium. She discovered a U.S. Mail Priority envelope, inside of which was what purported to be an IRS Notice addressed to C.M. demanding payment for "Fiduciary Taxes" in the amount of \$158,500.00 and directing the amount to be sent to Intel Realty Financial Services ("IRFS") or the PHH IRS Collection Services at 1783 Forest Drive, #339, Annapolis MD 21401. On June 17, 2010, P.H. contacted WHITE and inquired about the notice. WHITE told P.H. that she would have to pay the taxes as demanded by the notice. WHITE also told P.H. that she had received more notices, which she then faxed to P.H. from fax number 240-455-6491, which, according to records received from Comcast, is subscribed to Great White Bay, LLP at 1401 Mercantile Lane, Suite 200-C, Largo, Maryland 20774. The notices that were faxed to P.H. were dated from November 2007 and were addressed to C.M. and E.M., the deceased parent of C.M. WHITE also provided to P.H. a personal check that purportedly C.M. had used to pay some of

the taxes due before her illness; the check was written in the amount of \$10,250.00. As a result, P.H. obtained two Bank of America cashier's checks, check #382463 for the amount of \$34,375.00 and check #3824764 for the amount of \$17,738.00 and mailed them to the P.O. Box. These checks were drawn on a Bank of America account belonging to C.M. that P.H. had control over because she was appointed C.M.'s guardian.

16. Detective Renee Brown of the Anne Arundel County Police Department told me that pursuant to a subpoena that she had served regarding P.O. Box #339, the owner of the P.O. Box is IRFS, 1783 Forest Drive, #339, Annapolis, Maryland 20401. The P.O. Box was leased on June 4, 2010 by someone who identified themselves as C.M. The individual leasing the P.O. Box provided for identification a Howard University identification card and a Maryland Motor Vehicle Administration Title for a 1993 Volvo belonging to C.M. Detective Brown also told me that she confirmed through Howard University that the ID card was counterfeit. At the time the P.O. Box was leased, C.M. was incapacitated from a stroke and residing in a nursing facility. Based on this information and this investigation, your affiant believes that this P.O. Box was opened fraudulently with an individual falsely using the identity of C.M.

17. Your affiant advised P.H. that the P.O. Box, #339, in the name of IRFS, 1783 Forest Drive, Annapolis, Maryland 21401 was opened by someone claiming to be C.M. on June 4, 2010 and that individual used a Howard University Student Identification Card and C.M.'s 1993 Volvo title. P.H. told me that the title for C.M.'s Volvo was stored in C.M.'s condominium and that WHITE had access to the condominium. P.H. also advised your affiant that the vehicle title was given to her by WHITE who told her that she had found the title at C.M.'s condominium. P.H. was shown the copy of the Howard University ID Card that had been retained by the Post Office, and when she looked at the photograph, she exclaimed; "That's the

DJ, that's the DJ!" P.H. explained that the photograph on the ID card was that of the Disc Jockey ("DJ") that WHITE had hired to play music at WHITE's daughter's 25th birthday party. P.H. then showed your affiant a picture taken at the party. The picture appears to be the same individual pictured on the Howard ID card.

18. P.H. told me that up until January 2013, she continued to receive notices purportedly from the IRS making demands for more tax payments. Whenever P.H. would seek assistance from WHITE, WHITE told her that she must make the payments to the IRS and to send the payments to the Annapolis P.O. Box at 1783 Forest Drive, #339, Annapolis MD 21401.

19. P.H. also received the "IRS Notices" by fax, and they were faxed to P.H. from WHITE's office at 1401 Mercantile Lane, Suite 200-CC, Largo, Maryland 20774. This was evidenced by WHITE's fax number printed on the notices. According to records received from Comcast, the fax number 240-455-6491 is subscribed to Great White Bay, LLP at 1401 Mercantile Lane, Suite 200-C, Largo, Maryland 20774. The directory at 1401 Mercantile Lane lists 200-CC as belonging to: L. Sandra White, Attorney at Law Great White Bay, LLP. P.H. also advised that WHITE has recently moved from Suite 200-C to 200-CC.

20. In December of 2012, WHITE left a message on P.H.'s voicemail threatening P.H. and telling her that she could lose everything -- her house, car and telephone -- if she did not send money to the IRS via IRFS, 1783 Forest Drive, #339, Annapolis MD 21401. Your affiant listened to this voicemail.

21. White advised your affiant that, as of December 2012, the funds that were C.M.'s were now completely depleted, so P.H. accessed her own retirement funds and sent approximately \$12,000 to the IRFS at the Annapolis P.O. Box.

22. P.H. told your affiant that during the process of obtaining guardianship, WHITE told P.H. that she had learned that an unknown person had attempted to obtain a Maryland driver's license in C.M.'s name. However, the attempt was thwarted when officials at the MVA discovered the individual not to be C.M., WHITE said.

23. P.H. was shown a photocopy of the MVA printout of C.M.'s driver's license. P.H. was shown the photograph on the printout and stated that the picture was that of WHITE. P.H., who has possession of C.M.'s actual driver's license, provided that to investigators, and the picture is that of a different person than the picture on the MVA printout. P.H. had no knowledge that WHITE had attempted to obtain or had actually obtained a driver's license in C.M.'s name.

24. P.H. provided the original tissue copies of the cashier's checks that she sent to IRFS at 1783 Forest Drive, #339, Annapolis, Maryland 21401. P.H. advised your affiant that in January 2013, she requested from Bank of America a confirmation that the cashier's checks had been negotiated and also asked where they had been deposited. Bank of America stated that they were deposited into an account ending in the digits 9549 belonging to IRFS at Wells Fargo Bank. According to records received from Wells Fargo Bank, the account belonging to IRFS was opened by an individual using the name C.M., however, the address registered with the account is 1382 Mount Zion Marlboro Road, # 400, Lothian, Maryland 20711. This address is known to be a privately owned Post Office Box that is registered to WHITE. On March 8, 2013, your affiant and Detective Brown responded to 1382 Mt. Zion Marlboro Road, and identified the address as the business Waysons Corner Self-Storage. Your affiant obtained from Waysons Corner Self-Storage a Mailbox Rental Agreement signed by WHITE for the rental of mailbox #400.



25. Seventeen photographs received from Wells Fargo Bank pursuant to subpoena show WHITE making numerous ATM deposits and withdrawals from the individual account ending in 4028 held in the name C.M., and the IRFS business account ending in 9549. For example, on December 5, 2012, pursuant to a demand letter purportedly from the IRS, P.H. withdrew \$6,600 from her personal savings account and sent a cashier's check to IRFS. On December 6, 2012, a Digital Video Snapshot from a Wells Fargo Bank ATM shows WHITE making a \$6,600.00 deposit into the IRFS account ending in 9549. In addition, bank statements from Wells Fargo Bank for the IRFS account disclose payments to pay off vehicle loans for a Volvo and Ford. Your affiant has learned that WHITE owns a 2011 Volvo, and her daughter, Brittany White, owns a 2008 Ford. A check was also written off the IRFS account for a condominium settlement of \$21,000.00 in the name Brittany White. Numerous checks were written from the IRFS account to Brittany White. Also, checks were written from the IRFS account to the "PARRISH FAMILY TRUST," totaling: \$100,770.00. WHITE'S maiden name is PARRISH.

26. To date, the total amount of funds that PH sent to IRFS is \$792,473.05. Upon analysis of information provided by Wells Fargo Bank, pursuant to subpoena, the total amount of "available copy" of electronic transaction amounts deposited into IRFS accounts to the IRFS Wells Fargo Bank account from PH's cashier's checks is \$561,386.27.

27. P.H. told your affiant that she knows WHITE's law office to be located at 1401 Mercantile Lane, RM 200-CC, Largo, Maryland 20774. P.H. has visited WHITE there and knows her to conduct her law practice from that office.

28. P.H. also has been present at WHITE's home located at 4312 Arabella Court, Upper Marlboro, Maryland 20772. She has discussed this case with her there and knows her to maintain a home office at that location.

29. P.H. was not aware that WHITE was disbarred from practicing law in Maryland on September 9, 2011 and the District of Columbia in January 2011.

30. I know from my training and experience that criminals often utilize P.O. boxes and obtain them by stealing identities to conceal their identity and criminal scheme. Other than P.H., the only other person who had access to C.M.'s vehicle title was WHITE and/or her assistants whom WHITE had accompany her at different times while taking inventory of C.M.'s condominium. As discussed above, the photograph on the face of the Howard University ID card was that of an individual hired by WHITE. Both the ID card and the vehicle title were used to lease the P.O. Box just weeks before the first fraudulent IRS notice was received by P.H.

31. In addition, as the driver's license records on file with the Maryland MVA contain the picture of WHITE, it appears that WHITE has fraudulently obtained a license in C.M.'s identity.

32. I know from my training and experience conducting many impersonation investigations that criminals who impersonate the IRS and utilize fraudulent IRS documents do so because of the weight and gravity that the IRS embodies. The criminals involved in these schemes usually have some background in tax knowledge, such as in accounting or law, to assist them in preparing the documents. WHITE, a disbarred attorney, provided some of these fraudulent IRS notices directly to P.H.

33. I know from training and experience that persons operating fraudulent schemes often maintain information and items related to the scheme, at the location from which the

scheme is perpetrated. This place may be an office or a home and the person often transports and stores evidence, fruits and instrumentalities of the crime from the office to the home and vice versa. I also know from training and experience that in this modern technological environment, many times the line between office, home and vehicle is often blurred because of technology that allows persons to be mobile in their endeavors.

34. I know that WHITE is operating a business and law office at 1401 Mercantile Lane, RM 200-CC, Largo, Maryland 20774. I know that P.H. has met WHITE at that address for meetings that were directly related to this scheme. On the building directory, WHITE, L.SAUNDRA, Attorney at Law, is listed as the occupant for RM 200-CC. In addition, an employee of the Realty Service Company, the management company for 1401 Mercantile Lane, confirmed to your affiant that WHITE is leasing RM 200-CC.

35. I know that WHITE lives at 4312 Arabella Court, Upper Marlboro, Maryland 20772. P.H. has been present at WHITE's home and had discussions related to this scheme there. In addition, P.H. has told me that WHITE has a home office at her residence where she also conducts business. On March 19, 2013, your affiant observed a trash can on the street in front of 4312 Arabella Court. Your affiant was able to obtain a trash bag from that trash can and upon searching the discarded trash, located a discarded "Target Pharmacy" bag and prescription information. Located on the bag was a sticker with the name and address; SAUNDRA L. PARRISH-WHITE, 4312 Arabella Ct. Upper Marlboro, MD 20772.

#### **COMPUTERS, CELLULAR PHONES AND COMPUTER EQUIPMENT**

36. Based upon your affiant's knowledge and information received from other law enforcement officers, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to

be searched later by a qualified computer expert in a laboratory or other controlled environment.

This is true because:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he/she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such



searches often require the seizure of most or all of the computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

d. Variety of forms of electronic media. Records sought under this warrant could be in a variety of storage media formats, including cellular phones, that may require off-site reviewing with specialized forensic tools.

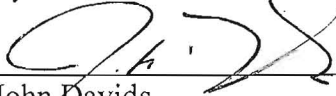
e. In light of these concerns, your Affiant hereby requests the Court's permission to seize the computer hardware, storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware, media, or peripherals on-site for this evidence.

f. Based on my experience in other investigations and information provided to me by other law enforcement officers, it is common for individuals to utilize computers and electronic peripherals in their residence for the purpose of booking travel, keeping ledgers and communicating with other members of the organization in furtherance of the money laundering and drug smuggling activities. I submit therefore that there is probable cause to believe that computers, storage media devices, cellular telephones and peripherals within "Target Locations," may contain evidence, fruits, and instrumentalities of the crime of money laundering and drug smuggling.

**CONCLUSION**

37. I have probable cause to believe that WHITE is using her business address of 1401 Mercantile Lane, RM 200-CC, Largo, Maryland 20774 and her home address of 4312 Arabella Court, Upper Marlboro, MD 20772, to conduct the above unlawful activity, and that a search of those premises will yield evidence, fruits and instrumentalities regarding these crimes.


38. Your affiant submits that there is probable cause to believe that WHITE has committed violations of wire fraud, a violation of Title 18, United States Code, Section 1343; misuse of Department of Treasury names and symbols, a violation of Title 31, United States Code, Section 333; and aggravated identity theft, a violation of Title 18, United States Code, Section 1028A, and that located at 1401 Mercantile Lane, RM 200-CC, Largo, Maryland 20774 (more fully described in Attachment A) and at 4312 Arabella Court, Upper Marlboro, MD 20772 (more fully described in Attachment B) will be found fruits, evidence, and instrumentalities of their violations, which are more particularly described in Attachment C.

  
\_\_\_\_\_

John Davids  
Special Agent

U.S. Treasury Inspector General for Tax Administration

Sworn to and Subscribed before me this 15<sup>th</sup> day of May 2013.

  
\_\_\_\_\_

The Honorable Jillyn K. Schulze  
United States Magistrate Judge  
Greenbelt, Maryland

**ATTACHMENT A**

**Property to Be Searched**

**1401 Mercantile Lane, Suite 200-CC, Largo, Maryland, 20774**

**Description:** Displayed on the top front of the office building are the numbers 1401 and below the numbers are glass windows down to the glass entrance doors. The office to be searched is located in Suite 200, on the second floor, directly to the right of the elevators. Suite 200 also contains numerous other businesses. Office 200-CC is located down the hallway directly to the right after entering Suite 200 and passing through a sitting area. Office 200-CC is identified by a brown door and to the left of the door is a sign that has the numbers 200-CC and directly below the words "Great White Bay, LLP."

**ATTACHMENT B**

**Property to Be Searched**

**4312 Arabella Court, Upper Marlboro, Maryland 20774**

**Description:** A two story, brick front single family residence located on the southeast corner of Arabella Court and Dunkirk Drive. The house has brown brick and cream trim, the numbers 4312 are attached on the fascia over the front door, and when facing the house from the street, there are two cream colored garage doors on the left side of the house.



**ATTACHMENT C**

**Particular Things to Be Seized**

Evidence and proceeds relating to bank fraud including the following:

1. All documents constituting or relating to identification documents, including driver's licenses, social security cards, visas, passports, permits, alien registration cards, membership cards, photo identification cards, and photographs capable of being used in any identification document;
2. Any machine, device, or materials used for the production of fraudulent identification documents or checks.
3. Any cellular telephone, pager, or fax machine, and all documents relating thereto, including billing statements, subscriber information, and call detail records;
4. All credit cards, debit cards, gift cards, or ATM cards, and all documents relating thereto, including credit card statements, applications, receipts, and any correspondence to or from any bank or credit card issuer;
5. All documents relating to any bank account, including bank statements, deposit slips, registers, check books, checks, check stubs, canceled checks, money orders, and wire transfer notices;
6. All documents relating to the creation, incorporation, or functioning of any corporation, partnership, or other entity;
7. Any pre-fabricated rubber stamps used to endorse checks;
8. All documents reflecting or relating to any financial transaction, including earnings or revenues, allocations of funds, division of proceeds, general journals and ledgers;
9. All documents containing names, addresses, personal identification information, credit card account numbers, credit card balances, credit card limits, bank account numbers, and bank account balance statements;
10. All documents constituting or relating to any address book, diary, or calendar, including any book, paper, log, or other item used to record or store names, addresses, telephone numbers, appointments, or events;
11. All cash or currency of any kind;
12. All documents referring or relating to the location of any cash or funds, including any safe deposit box or keys.

13. Any items of U.S. Mail addressed to C.M., IRFS, the IRS or to any individuals or entities other than the verifiable owners and occupants of the residence to be searched;

14. Search and seize any and all bank records, documents and materials relating to: C.M., IRFS, the IRS and any other names not associated with the occupants of the residence to be searched;

15. All documents constituting or relating to any income tax return, W-2 form, 1099 form, K-1 form, schedule, and related tax information;

16. Any documents related to the renting of a Post Office Box;

17. Any computer hardware, including file servers, desktop computers, laptop computers, mainframe computers; electronic, magnetic or digital storage devices such as hard drives, zip drives, CD-ROMs, floppy disks, and any other electronic media storage device; any internal and external peripheral devices (e.g. printers, scanners) and any of the above listed records, documents or materials which are maintained on computer located at the premises, to include the device, (computer), wherein these records, documents or materials are maintained, for search as detailed in the affidavit;

18. Computer passwords and other data security devices necessary to gain access to any computer equipment or electronic storage devices seized during the search;

19. Any door, safe, locked boxes or receptacles where the aforementioned items could be hidden.

To effectuate the search and to the extent necessary retrieve responsive documents which may be stored electronically, the following items will be seized as needed:

a. Hardware:

Computer hardware consisting of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computerized impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, disk drives and diskettes, tape drivers and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); cellular telephones (including personal digital assistants (PDAs), smart phones, and tablets); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communication devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or part that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Documentation:

Computer-related documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

c. Software:

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communication programs.

d. Passwords and Data Security Devices:

Computer passwords and any other data security devices are designed to restrict access or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

The terms “records,” “documents,” and “materials” include all of the following items of evidence in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications may have been created and stored, including but not limited to: any handmade form (such as writing or drawing with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); and any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs or any information on an electronic or magnetic storage device, such as floppy discs, compact discs, hard disks or drives, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drivers, cellular telephones, personal digital assistants (PDAs), smart phones, tablets, or electronic notebooks, as well as printouts or readouts from any magnetic storage device.